

# United States District Court

RECEIVED  
U.S. DISTRICT COURT, SCDISTRICT OF South Carolina

2006 AUG 14 A 10:13

UNITED STATES OF AMERICA

V.

**Jonathan Giannone****CRIMINAL COMPLAINT**CASE NUMBER: 3:06cr 849

(Name and Address of Defendant)

I, the undersigned complainant being duly sworn state the following is true and correct to the best of my knowledge and belief. On or about May - June 2005 in Lexington county, in the \_\_\_\_\_ District of South Carolina, defendant(s) did, (Trace Statutory Language of Offense)

devise a scheme to defraud by transmitting data over the internet, via computer, for the purpose of obtaining money and property by means of fraudulent pretenses.

in violation of Title 18, United States Code, Section(s) 1343.

I further state that I am a(n) Special Agent - USSS and that this complaint is based on the following facts:

Official Title

**See attached affidavit.**

Continued on the attached Sheet and made a part hereof:

☒ Yes ☐ No

[Signature]  
Signature of Complainant

Sworn before me and subscribed in my presence,

August 14, 2006  
Date

at

Columbia, SC  
City and State

**Bristow Marchant - U.S. Magistrate Judge**

Name and Title of Judicial Officer

[Signature]  
Signature of Judicial Officer

**AFFIDAVIT**RECEIVED  
2006 AUG 14 COLUMBIA, SC

Bobby J. Kirby, being first duly sworn, hereby states as follows:

2006 AUG 14 A 10: 13

1. Your affiant is a Special Agent with the United States Secret Service, Columbia Field Office, and has been employed in this capacity since February 2003. Your affiant's responsibilities include the investigation of fraud and related activity in connection with access devices.
2. On May 19, 2005 the Columbia Field Office, United States Secret Service, initiated Operation Anglerphish. This investigation utilized a confidential informant (CI) and targeted organized criminal groups dedicated to promoting malicious computer hacking; Internet fraud schemes; electronic theft of personal financial and identifying information; trafficking in and use of stolen credit card and debit card information ("dumps"), stolen bank account information, and other stolen individual identifying information; and the production of, trafficking in, and use of counterfeit identification documents. Internet web sites, such as forum.theftservices.com and scandinaviancarding.com, are the public manifestations of the criminal organizations which serve primarily as communications media to facilitate the commission of the above-referenced criminal activity. These web sites publicly disseminate information regarding the perpetration of such criminal activity through postings and responses to postings by members to electronic forums on the sites. They also facilitate the transmission and receipt of private electronic messages between members of the criminal organizations. Furthermore, the web sites serve as electronic bulletin boards for members of the criminal organizations to advertise and promote the sale of credit card and debit card dumps, stolen bank account information, other stolen individual identifying information, and counterfeit identification documents to other members.
3. The criminal organizations operate their associated web sites and oversee the activities of their members through the following hierarchical framework:
  - a. **Administrators/Forum Techs** are a small group of individuals that serve as a governing council of each criminal organization who, collectively, control the destiny of their organization. The administrators handle day-to-day management decisions of the organizations as well as long-term strategic planning for their continued viability. They determine which individuals are permitted to become and remain members of criminal organizations; the functions, responsibilities and levels of access to information for all members of the organizations; and the rewards accorded members for their loyalty to the organizations as well as the punishments meted out to members evidencing disloyalty to the organizations. Furthermore, they decide when, how and under what circumstances to attack and/or to retaliate against members of rival criminal organizations and their associated Internet web

h

sites. The administrators are accorded full access to and privileges on the computer servers hosting the corresponding web sites and, thus, had ultimate responsibility for the physical administration, maintenance and security of these computer servers as well as for the content of the web sites.

- b. **Moderators** oversee and administer one or more subject-matter-specific forums on the web sites that either fall within an area of their expertise or cover their geographic location, limiting their activities to editing and deleting posts by members on these forums. Moderators also frequently serve as reviewers for particular products or services with which they have an expertise.
- c. **Reviewers** examine and/or test products and services that members of the criminal organizations desire to advertise and sell via the corresponding web sites (e.g. counterfeit passports, drivers licenses, Social Security cards, credit cards, birth certificates and other identification documents; credit card dumps; counterfeit checks; and stolen credit card pre-authorization (“dump check”) services) and post a written summary of that examination or testing on the appropriate web site. A favorable written review is a prerequisite to vending on the web sites hosted by the criminal organizations. While most reviewers primarily serve in the capacity of administrator or moderator, any qualified individual can be appointed by an administrator to conduct a review, even a general member.
- d. **Vendors** advertise and sell products and services to members of the criminal organizations via the associated web sites after the product or service has received a favorable written review from a reviewer. Once a reviewer was designated, a prospective vendor is required to ship multiple samples of the product or provide access to the service to facilitate completion of the review. This contact between the prospective vendor and the reviewer is usually made through a private e-mail message or through a public post in a forum on the relevant web site.
- e. **General members** of the criminal organizations have no role in the operation of the corresponding web sites. Instead, they typically use the web sites to gather and provide information about perpetrating criminal activity through postings on the various forums and through private e-mail messaging to other members. They also use the sites to facilitate their purchases of credit card dumps, false identification documents and other contraband that then serves as instrumentalities of their own criminal conduct. A member of any of these criminal organizations is known to other members by his/her chosen screen name or nickname (“nic”). Individuals often are known by and conduct their criminal business under more than one nic. The use of these nicknames facilitates the member’s anonymity in conducting their illegal activity.

87

4. The continued viability of the criminal organizations is dependent upon individuals who are skilled hackers. A computer hacker is an individual who accesses computer systems without authorization, often for the purpose of stealing information or causing damage to computer systems. Hackers, whether actual members of the criminal organizations or not, are the primary source of credit card dumps and stolen identity information that are sold on the associated web sites and used to create false identity documents and counterfeit credit cards. Like the members of the criminal organizations that they service, hackers are known by their nic's and predominantly communicate with each other and with others in the online criminal underworld through real-time chat sessions, exchanging information on forums and other electronic bulletin boards, and private e-mail messaging.
5. The hackers and members of the criminal organizations use their own descriptive vernacular when communicating with each other regarding their criminal activity. Several of the most frequently used words and phrases include:
  - a. **"Carding"** refers to the general concept of purchasing retail items with counterfeit credit cards or stolen credit card information.
  - b. **"Change of billing"** (or cob) occurs when an individual, after having acquired all the pertinent information related to victim's credit card account, accesses the account via the Internet or via a telephone call and causes the billing address for the credit card to be changed, or causes an alternate shipping address to be added, in order to facilitate credit card fraud.
  - c. **"Phishing"** refers to an Internet fraud scam involving the sending out of large volumes of unsolicited commercial e-mail ("spam") containing a link to a replica of an Internet web page of a well known commercial or financial company in an effort to trick the victim into clicking on this link and entering his/her credit card or personal financial information as requested by the replica web page which is then sold by the offender or used by the offender to commit fraud or identity theft.
6. The informant utilized by the Columbia Field Office, hereafter Brett Johnson, had established a well recognized nickname, "gollumfun", throughout the online community by serving as an administrator, moderator and reviewer on several web sites, to include [www.counterfeitlibrary.com](http://www.counterfeitlibrary.com) and [www.shadowcrew.com](http://www.shadowcrew.com). These sites are no longer active. Brett Johnson used his nickname to gain access to current web pages and forums and communicate with people actively engaged in fraudulent activity. The web pages targeted by this investigation have included [forum.theftservices.com](http://forum.theftservices.com), [www.scandinaviancarding.com](http://www.scandinaviancarding.com) and [www.mazafaka.cc](http://www.mazafaka.cc).
7. Brett Johnson was removed from his position as a Confidential Informant (CI) with this office upon the determination that Johnson was engaged in fraudulent activities during his time as a CI. Johnson also divulged sensitive information

R

regarding his work to unauthorized individuals. Currently, Johnson is a fugitive with an outstanding Federal arrest warrant and an outstanding state bench warrant. All activities described herein which are attributed to Johnson were monitored by Agents of the U.S. Secret Service, Columbia Field Office.

8. The members of these criminal web sites have employed multiple, real-time Internet chat messaging services to facilitate the commission of criminal conduct. These services include AIM (America Online Instant Messenger), ICQ (I seek you), mIRC (Internet Relay Chat), Yahoo Messenger, and the MSN (MicroSoft Network). Many of these chat messaging services can all be accessed simultaneously using a software program called Trillian, which offers features such as encrypted instant messaging capabilities. These services accommodate discussions among the subjects and aid them in securing their communications with each other. Specifically, Trillian offers a secure method by which online criminals can communicate and facilitates their ability to engage in criminal activity without being monitored by law enforcement.
9. During the course of this investigation, Brett Johnson communicated online with an individual using the screen names "Pit Boss 2600" and "CIA INTEL". During the course of this investigation, this "Pit Boss 2600" and "CIA INTEL" would communicate with Johnson using either of the two screen names. Based on the conversations, it is evident that the same person is using both screen names.
10. On 05/26/05, Brett Johnson was contacted online, via AIM, by an individual using the screen name "Pit Boss 2600". During this conversation, different fraudulent schemes were discussed and "Pit Boss 2600" sent five (5) Bank of America Platinum credit card numbers with associated cardholder names to Johnson. "Pit Boss 2600" went on to explain how to encode these account numbers on the magnetic stripe of a blank credit card. As he explained to Johnson how to create the Track 1 data, "Pit Boss 2600" realized that one of the cards had expired and sent another card number to replace it. "Pit Boss 2600" sent these numbers to Johnson with the understanding that he could use these as a sample. If Johnson was able to successfully make purchases with these numbers, Johnson would then purchase several more credit card numbers from "Pit Boss 2600".
11. On 05/31/05, SA Brad Smith, Columbia Field Office, contacted Todd Abbott, Bank of America, to verify the legitimacy of the account numbers referenced in paragraph 10. Abbott advised that these accounts were Texas personal check cards, but that they had been purged from their system and were not active any longer.
12. On 05/31/05, Johnson communicated again with "Pit Boss 2600" via AIM. Johnson informed "Pit Boss 2600" that all of the card numbers he had supplied on 05/26/05 were invalid. In response, "Pit Boss 2600" electronically sent three (3) additional credit card numbers to Johnson.

13. On 06/02/05, SA Brad Smith contacted Todd Abbott, Bank of America, to verify the legitimacy of the three (3) accounts received on 05/31/05. Abbott confirmed that these were legitimate accounts and currently active, one with an available balance of over \$20,000.00. Abbott added that these were also Texas personal check cards.
14. On 06/04/05, Johnson contacted "CIA INTEL" (aka "Pit Boss 2600") via AIM and told him that the last three (3) cards he sent were successful. "CIA INTEL" stated that he had twenty-one (21) additional cards and was willing to sell them all for \$600.00. As payment, "CIA INTEL" requested Johnson to deposit \$600.00 into a Fleet/Bank of America business account that "CIA INTEL" had set up as a fictitious corporation. "CIA INTEL" provided the following account information:

Fleet/Bank of America  
Account #: 9505552565  
A&W Auto Clinic  
395 Maple Street  
Holyoke, MA 01040

Johnson agreed to make the deposit in exchange for the twenty-one (21) account numbers.

15. On 06/06/05, "CIA INTEL" (aka "Pit Boss 2600") sent, via AIM, twenty-one (21) Bank of America Platinum debit cards.
16. On 06/07/05, Johnson made a \$600.00 deposit into account # 9505552565 at The Bank of America located at 301 Harbison Boulevard, Columbia, SC 29212, at 1:26 PM. Johnson then contacted "CIA INTEL", via AIM, later that day and confirmed that the money had been deposited. "CIA INTEL" confirmed that the deposit had been credited to his account.
17. An initial inquiry into business account number 9505552565 revealed that it was associated to a personal account, account number 9494910645, through a common telephone number in the account application.
18. On 07/01/05, SA Brad Smith, Columbia Field Office, served a Grand Jury Subpoena on Bank of America, 5701 Horatio Street, Utica, NY 13502. This subpoena requested account holder information and statements from 01/01/05 through 06/10/05 for account numbers 9494910645 and 9505552565. Records provided to this Service, pursuant to the subpoena, indicated that account number 9494910645 was opened by Jonathan Giannone, 734 Franklin Ave, #421, Garden City, NY 11530. Account number 9505552565 was also opened in New York, but the address given for the business was 395 Maple Street, Holyoke, MA 01040.

22



19. Further review of the account records show a deposit of \$600.00 into account number 9505552565 on 06/07/05 and a withdrawal, the same day, of \$500.00 at an ATM located at 152 N. Village Avenue, Rockville Center, NY.
20. On 07/05/05, SA Bobby Kirby served a Grand Jury Subpoena on Bank of America, 2059 North Lake Parkway, Tucker, GA 30084. This subpoena requested account statements and account holder information for the twenty-four (24) account numbers sent to Johnson from "CIA INTEL." Records provided to this Service, pursuant to the subpoena, indicated that five (5) of the account numbers were not on file. The remaining nineteen (19) were current and active accounts that had a cumulative available balance of \$132,327.17.
21. On 02/09/06, a letter was forwarded to Janice Davis, Bank of America, to request that they determine if any fraudulent charges had occurred on the twenty-four (24) account numbers given to Johnson from "CIA INTEL."
22. On 02/27/06, Janice Davis provided information indicating that five (5) of the accounts had reports of fraudulent activity in the total amount of \$12,546.92.
23. On 07/24/06, SA Jason Byrnes and SA Scot Bryan, Manchester Resident Office, interviewed Hunter Moore, an associate of Giannone and a former confidential informant, regarding online names used by Giannone. Moore stated that Giannone used the online identity of "Pit Boss 2600" while they were associates.
24. On 08/04/06, SA Brad Smith, Columbia Field Office, received the opening documentation and signature cards for Bank of America account # 9505552565, discussed in paragraphs 14 and 16-19, from Mary Rogalski, Bank of America Legal Order Processing. This information was received pursuant to a Grand Jury Subpoena. This account was opened by Jonathan Giannone on 04/15/05 at Bank of America, 152 N. Village Avenue, Rockville Centre, NY 11570. The New York state driver's license used to open the account was license number 257064728, which was issued to Jonathan Giannone. The Bank of America employee who opened the account was Deborah Aluzzo.
25. On 08/07/06, SA Brad Smith contacted Deborah Aluzzo, Bank of America, to discuss her knowledge of the bank account and the account holder. Aluzzo stated that she remembered opening the account and would be able to recognize the account holder.
26. On 08/10/06, SA Hari Notani of the New York Field Office presented Deborah Aluzzo, Bank of America, a photo line-up containing a picture of Jonathan Giannone. Aluzzo positively identified the picture of Giannone as the individual who opened the A&W Auto Clinic bank account, account number 9505552565, on 04/15/05.

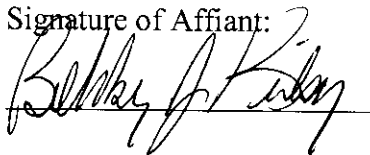
**Probable Cause**

rw

27. In support of this application, I submit that probable cause exists for the arrest of Jonathan Giannone for violation of Title 18 U.S.C. 1343 (Fraud by wire, radio or television) is as follows:
- a. Jonathan Giannone has been identified through bank records and an associate as the person using the screen name "Pit Boss 2600." Giannone also used the screen name "CIA INTEL" in his communications with Brett Johnson.
  - b. The Bank of America employee who opened the A&W Auto Clinic account on 04/15/05 positively identified Giannone in a photo line-up as the individual who opened the account.
  - c. Giannone sent Brett Johnson twenty-four (24) Bank of America account numbers, not issued or associated to him, via the instant message client AIM.
  - d. Bank of America confirmed that nineteen (19) of the twenty-four accounts were valid and had an available balance of \$132,327.17.

This affidavit, and the facts therein, have been approved by AUSA Dean Eichelberger, Columbia Division.

Signature of Affiant:

A handwritten signature in cursive script, appearing to read "Bobby J. Kiley", written over a horizontal line.

W